UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

7380 7590 08/25/2010

SMART & BIGGAR
P.O. BOX 2999, STATION D
900-55 METCALFE STREET
OTTAWA, ON K1P 5Y6
CANADA

EXAMINER	
AGWUMEZIE, CHARLES C	
ART UNIT	PAPER NUMBER
3685	

DATE MAILED: 08/25/2010

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/702,540	11/07/2003	Vincent So	79865-5 /ABA	8250

TITLE OF INVENTION: INTERNET-BASED DATA CONTENT RENTAL SYSTEM AND METHOD

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	11/26/2010

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

7380 7590 08/25/2010

SMART & BIGGAR
P.O. BOX 2999, STATION D
900-55 METCALFE STREET
OTTAWA, ON K1P 5Y6
CANADA

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/702,540	11/07/2003	Vincent So	79865-5 /ABA	8250

TITLE OF INVENTION: INTERNET-BASED DATA CONTENT RENTAL SYSTEM AND METHOD

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	11/26/2010

EXAMINER	ART UNIT	CLASS-SUBCLASS
AGWUMEZIE, CHARLES C	3685	705-059000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☐ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

☐ A check is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/702,540	11/07/2003	Vincent So	79865-5 /ABA	8250

7380 7590 08/25/2010

SMART & BIGGAR
P.O. BOX 2999, STATION D
900-55 METCALFE STREET
OTTAWA, ON K1P 5Y6
CANADA

EXAMINER	
AGWUMEZIE, CHARLES C	
ART UNIT	PAPER NUMBER
3685	

DATE MAILED: 08/25/2010

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 620 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 620 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Notice of Allowability	Application No.	Applicant(s)	
	10/702,540	SO, VINCENT	
	Examiner	Art Unit	
	CHARLES C. AGWUMEZIE	3685	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *communication filed on June 9, 2010*.

2. ☐ The allowed claim(s) is/are *1,4-23,34-36 and 38-56*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date See Continuation Sheet
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Charlie C Agwumezie/
Primary Examiner, Art Unit 3685
August 12, 2010

Continuation of Attachment(s) 3. Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date: 11/07/2003; 09/28/2007.

DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Jeffrey F. Slatter on August 12, 2010

2. The Application has been amended as follows:

1. (Previously Presented) A method of delivering data content from a data content provider to a customer processing platform and controlling use of the data content at the customer processing platform, comprising:

encrypting each of a plurality of sections of the data content using a respective one of a plurality of encryption keys to produce a corresponding plurality of encrypted sections;

delivering the plurality of encrypted sections to the customer processing platform; and

delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time, wherein delivering the plurality of decryption keys comprises:

delivering to the customer processing platform a current key of the plurality of decryption keys;

delivering to the customer processing platform a next key of the plurality of decryption keys; and

causing the current key to be destroyed at the customer processing platform only after at least the next key of the plurality of decryption keys has been received.

2. (Cancelled)

3. (Cancelled)

4. (Previously Presented) The method of claim 1, wherein delivering to the customer processing platform a next key of the plurality of decryption keys and causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections to be subsequently processed.

5. (Previously Presented) The method of claim 1, wherein the current encrypted section is a first one of the plurality of encrypted sections, and wherein delivering to the customer processing platform a next key of the plurality of decryption keys and causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections following the first encrypted section.

6. (Previously Presented) The method of claim 1, wherein delivering to the customer processing platform a plurality of decryption keys comprises:

providing key control software to the customer processing platform, the key control software being adapted to:

receive the current decryption key for the current encrypted section of the plurality of encrypted sections;

receive the next decryption key for the next encrypted section of the plurality of encrypted sections;

complete decryption of the current section;

begin decryption of the next section; and

destroy the current decryption key after decryption of the next section has begun.

7. (Original) The method of claim 1 further comprising:

billing a customer for delivery of the encrypted sections, and then billing the customer each time the data content is used at the customer processing platform.

8. (Original) The method of claim 1, wherein the data content is video content or music content, and wherein use of the data content at the customer processing platform comprises decryption and playback of the data content.

9. (Original) The method of claim 1, wherein each of the plurality of encryption keys comprises a respective symmetric cryptographic key, and wherein each of the plurality of decryption keys comprises the symmetric cryptographic key of its corresponding encryption key.

10. (Original) The method of claim 1, further comprising:

generating each of the plurality of encryption keys using an identifier associated with the customer processing platform, to thereby generate a plurality of customer processing platform-specific keys.

11. (Original) The method of claim 10, wherein generating comprises generating each of the plurality of customer processing platform-specific keys using the identifier and a respective key generation seed value.

12. (Original) The method of claim 11, wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the respective key generation seed values.

13. (Original) The method of claim 1, further comprising:

generating a respective transmission value for each of the plurality of encryption keys using an identifier associated with the customer processing platform,

wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the transmission values.

14. (Previously Presented) The method of claim 1, further comprising:

delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform via a peer-to-peer network; and

delivering the plurality of decryption keys from the data content provider to the second customer processing platform, wherein the decryption keys are delivered in a manner such that the second customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time, wherein the plurality of decryption keys are encrypted using a public cryptographic key corresponding to a private cryptographic key known only to the customer processing platform.

15. (Original) A computer-readable medium storing instructions which, when executed by a processor at a data content provider, perform a method according to claim 1.

16. (Currently Amended) A method of receiving and controlling playback of video data content at a customer processing platform, comprising:

the customter processing platform performing steps of:

receiving over a communications medium a plurality of encrypted sections of video data content, each of which has been encrypted using a respective encryption key; and

for each encrypted section:

receiving a respective decryption key in respect of the encrypted section before playback of a preceding encrypted section of the plurality of encrypted sections is complete;

decrypting and playing back the encrypted section using the respective decryption key; and

destroying the respective decryption key only after at least a respective decryption key in respect of a next encrypted section has been received, such that contiguous playback of the encrypted sections of video data content is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of video data content.

17. (Previously Presented) The method of claim 16, further comprising, for each encrypted section:

destroying decrypted video data content at the customer processing platform after completing playback of the encrypted section.

18. (Original) The method of claim 16, wherein the communications medium is the public Internet.

19. (Previously Presented) The method of claim 16, wherein, for each encrypted section, the respective encryption key is the same as the respective decryption key.

20. (Previously Presented) The method of claim 16, wherein receiving the plurality of encrypted sections of the video data content comprises receiving the plurality of encrypted sections of the video data content from another customer processing platform via a peer-to-peer network, and wherein, for each encrypted section, the decryption key is encrypted using a public cryptographic key corresponding to a private cryptographic key known only to the customer processing platform.

21. (Original) A computer-readable medium storing instructions which, when executed by a customer processing platform, perform a method according to claim 16.

22. (Original) The method of claim 16, wherein each encryption key comprises a respective customer processing platform-specific key which is determined based on an IP address of the customer processing platform.

23. (Previously Presented) The method of claim 16, wherein receiving each respective decryption key comprises receiving a transmission value that is determined based on the respective decryption key and a hardware identifier associated with the customer processing platform, further comprising, for each encrypted section:

recovering the respective decryption key from the transmission value.

24.–33.(Cancelled)

34. (Previously Presented) A method for controlling use of encrypted video data content downloaded to a customer data content processing device, comprising:

receiving a request comprising customer verification information from a customer data content processing device;

comparing the customer verification information with corresponding stored customer information; and

where the customer verification information is consistent with the stored customer verification information:

billing a usage charge to an account of the customer;

transmitting to the customer data content processing device a digital key to decrypt a current portion of the encrypted video data content; and

for each subsequent portion of the encrypted video data content:

transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted video data content before playback of a preceding portion of the encrypted video data content is complete; and

causing a key for a preceding portion of the encrypted video data to be deleted from the customer data content processing device only after at least the key to decrypt the subsequent portion of the encrypted data has been received by the customer data content processing device, such that contiguous playback of the portions of encrypted video data content is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the encrypted video data content.

35. (Currently Amended) A computer readable medium storing software code executable by a processing platform that when executed by the processing platform cause the processing platform to perform a method[[, the software code]] comprising:

[[first software code for]]coordinating downloading a plurality of sections of data content each encrypted with a respective one of a plurality of encryption keys to a customer computer system from a data content service provider system or another customer computer system; [[and]]

[[second software code for]]establishing a connection with the data content service provider system to obtain permission to use the data content[[,]]; and [[for]]

using the data content where permission is obtained from the data content service provider system by receiving a corresponding one of a plurality of decryption keys for each encrypted section of data content and decrypting the encrypted section using the corresponding one of the plurality of decryption keys such that the processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time,

wherein for each encrypted section of data content the [[second software code]]processing platform destroys the received decryption key corresponding to the encrypted

section of data content only after receiving at least the decryption key corresponding to the next encrypted section of data content.

36. (Currently Amended) The computer readable medium of claim 35, wherein the [[second software code]] processing platform obtains further permissions from the data content service provider system to continue using the data content.

37. (Cancelled)

38. (Previously Presented) A system for delivering data content from a data content provider to a customer processing platform and controlling use of the data content at the customer processing platform, comprising:

means for encrypting each of a plurality of sections of the data content using a respective one of a plurality of encryption keys to produce a corresponding plurality of encrypted sections;

means for delivering the plurality of encrypted sections to the customer processing platform; and

means for delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time, wherein the means for delivering the plurality of decryption keys comprises:

means for delivering to the customer processing platform a current key of the plurality of decryption keys; and

means for delivering to the customer processing platform a next key of the plurality of decryption keys,

the customer processing platform comprising:

means for destroying the current key at the customer processing platform only after at least the next key of the plurality of decryption keys has been received.

39. (Previously Presented) The system of claim 38, wherein the customer processing platform comprises:

means for requesting the data content to be delivered to the customer processing platform via a peer-to-peer network connection;

means for receiving the plurality of encrypted sections via the peer-to-peer network connection;

means for receiving, for each encrypted section, the decryption key in respect of the encrypted section over an encrypted decryption key delivery channel; and

means for decrypting and playing back the encrypted section using the decryption key, wherein

the means for destroying the current decryption key comprises means for destroying the current decryption key, after completing playback of the current encrypted section and beginning playback of the next encrypted section.

40. (Currently Amended) A data content distribution system comprising:

a data content server [[configured to]]that receives download requests and permission requests for data content, [[to]]that encrypts a plurality of sections of requested data content using respective encryption keys to thereby generate a plurality of encrypted sections and [[to]]that transmits the encrypted sections of the data content in response to a received download request for the data content, and [[to]]that transmits each of a plurality of decryption keys respectively corresponding to the encryption keys in response to a permission request for the data content; and

a data content download controller [[configured to]]that generates download requests, [[to]]that receives encrypted sections of data content in response to download requests, [[to]]that generates permission requests when downloaded data content is to be used, and for each encrypted section of data content to be used, [[to]] receives a corresponding one of the plurality of decryption keys, and [[to]]that decrypts the encrypted section using the corresponding one of the plurality of decryption keys;

wherein said data content server [[operable to]] transmits the plurality of decryption keys in a manner such that the data content download controller has simultaneous possession of at most a subset of the plurality of decryption keys at any time, wherein, for each encrypted section, the data content download controller destroys the decryption key corresponding to the encrypted section only after at least the decryption key corresponding to the next encrypted section of the plurality of encrypted sections has been received.

41. (Original) The system of claim 40, comprising a data network connecting the data content server and the data content download controller.

42. (Original) The system of claim 41, further comprising a plurality of data content download controllers connected to the data network.

43. (Currently Amended) The system of claim 42, wherein each of the plurality of data content download controllers is implemented in conjunction with a respective customer computer system and each data content download controller [[is further configured to]] downloads encrypted sections of data content from other customer computer systems.

44. (Previously Presented) The method of claim 1, wherein causing the current key to be destroyed at the customer processing platform comprises:

causing the current key to be destroyed at the customer processing platform after processing of the current encrypted section of the plurality of encrypted sections with the current key has been completed and processing of a next encrypted section of the plurality of encrypted sections with the next key has begun.

45. (Previously Presented) The method of claim 1, wherein causing the current key to be destroyed at the customer processing platform comprises:

causing the current key to be destroyed at the customer processing platform before processing of the next encrypted section has been completed.

46. (Previously Presented) The method of claim 1, wherein:

delivering to the customer processing platform a plurality of decryption keys comprises:

delivering the plurality of decryption keys to the customer processing platform over an encrypted decryption key delivery channel; and

delivering the plurality of encrypted sections to the customer processing platform comprises:

providing the plurality of encrypted sections to a peer-to-peer network, wherein the customer processing platform downloads the plurality of encrypted sections via the peer-to-peer network.

47. (Previously Presented) The method of claim 34, wherein causing a key for a preceding portion of the encrypted data to be deleted comprises:

causing the key for the preceding portion of the encrypted data to be deleted from the customer data content processing device only after decryption of the subsequent portion of the encrypted data has begun.

48. (Currently Amended) The computer readable medium of claim 35, wherein the [[second software code]]processing platform destroys the received decryption key corresponding to the encrypted section of data content only after decryption of the next encrypted section of data content has begun.

49. (Previously Presented) The system of claim 38, wherein the means for causing the current key to be destroyed at the customer processing platform comprises:

means for causing the current key to be destroyed at the customer processing platform after processing of the current encrypted section of the plurality of encrypted sections with the current key has been completed and processing of a next encrypted section of the plurality of encrypted sections with the next key has begun.

50. (Previously Presented) The system of claim 38, wherein the means for causing the current key to be destroyed at the customer processing platform comprises:

means for causing the current key to be destroyed at the customer processing platform before processing of the next encrypted section has been completed.

51. (Previously Presented) The system of claim 38, wherein:

the means for delivering to the customer processing platform a plurality of decryption keys comprises:

means for delivering the plurality of decryption keys to the customer processing platform over an encrypted decryption key delivery channel; and

the means for delivering the plurality of encrypted sections to the customer processing platform comprises:

a peer-to-peer network, wherein the customer processing platform downloads the plurality of encrypted sections via the peer-to-peer network.

52. (Previously Presented) The system of claim 40, wherein the data content download controller destroys the decryption key corresponding to the encrypted section only after decryption of the encrypted section has completed and decryption of the next encrypted section of the plurality of encrypted sections with the decryption key corresponding to the next encrypted section of the plurality of encrypted sections has begun.

53. (Previously Presented) The system of claim 43, comprising an encrypted decryption key channel for delivery of the plurality of decryption keys, wherein the data network comprises a peer-to-peer network connecting the customer computer systems to share the encrypted sections of data content, and wherein the encrypted decryption key channel is separate from the peer-to-peer network.

54. (Previously Presented) The method of claim 16, wherein destroying the respective decryption key only after at least the respective decryption key in respect of the next encrypted section has been received comprises destroying the respective decryption key only after completing playback of the encrypted section and beginning contiguous playback of the next encrypted section.

55. (Previously Presented) The method of claim 16, further comprising, for each encrypted section:

requesting the respective decryption key in respect of a next encrypted section responsive to one of a control signal and a data pattern in the decrypted data content of an encrypted section that precedes the next encrypted section.

56. (Previously Presented) The method of claim 34, further comprising, for each subsequent portion of the encrypted data:

receiving a request from the customer data content processing device for the different key to decrypt the subsequent portion of the encrypted data, wherein the request was generated responsive to one of a control signal and a data pattern in the decrypted data content of a preceding portion of the encrypted data content during playback of the preceding portion of the encrypted data content.

Rejoinder of Previously Withdrawn claims

3. Claims 1, 4-23, 34-36, and 38-56 directed to an allowable product. Pursuant to the procedures set forth in MPEP § 821.04(B), claim1, 4-15, 35-36, and 38-53, directed to the process of making or using an allowable product, previously withdrawn from consideration as a result of a restriction requirement, claims 1, 4-15, 35-36, and 38-53 is hereby rejoined and fully examined for patentability under 37 CFR 1.104.

Because all claims previously withdrawn from consideration under 37 CFR 1.142 have been rejoined, **the restriction requirement as set forth in the Office action mailed on June 30, 2008 is hereby withdrawn**. In view of the withdrawal of the restriction requirement as to the rejoined inventions, applicant(s) are advised that if any claim presented in a continuation or divisional application is anticipated by, or includes all the limitations of, a claim that is allowable in the present application, such claim may be subject to provisional statutory and/or nonstatutory double patenting rejections over the claims of the instant application. Once the restriction requirement is withdrawn, the provisions of 35 U.S.C. 121 are no longer applicable. See *In re Ziegler*, 443 F.2d 1211, 1215, 170 USPQ 129, 131-32 (CCPA 1971). See also MPEP § 804.01.

Reasons for Allowance

The following is an examiner's statement of reasons for allowance:

4. Regarding the claimed terms, the Examiner notes that a "general term must be understood in the context in which the inventor presents it." In re Glaug F.3d 1335, 1340, 62 USPQ2d 1151, 1154 (Fed. Cir. 2002). Therefore the Examiner must interpret the claimed terms as found on pages 1-35 of the specification. Clearly almost all the general terms in the claims may have multiple meanings. So where a claim term "is susceptible to various meanings, … the inventor's

lexicography must prevail...." Id. Using these definitions for the claims, the claimed invention was not reasonably found in the prior art.

The closest prior art of record is Feig et al, U.S. Patent No. 7,251,833.

The primary reference Feig et al. (U.S. Patent No. 7,251,833) describes a method for enforcing the sequential playback of a multimedia file by partitioning the media file into a plurality of sequential data blocks, encoding each respective one of the sequential data blocks with a corresponding one of a plurality decryption keys, transferring the encoded sequential data blocks to a receiving client, and streaming a plurality of decryption keys to the receiving client. Feig et al. teaches that the decryption keys are streamed one at a time to the client to enforce sequential playback of the media file, but fails to describe any mechanism for preventing the client from retaining all of the decryption keys and all of the decrypted content once all of the decryption keys have been delivered to the client.

Giroux et al. teaches an information security architecture for encrypting and distributing a segment of electronic information for remote access while maintaining access control to the encrypted electronic information by dispensing decryption keys for the encrypted electronic information via a remote server 106 to an authorized user 116, and causing the user's decryption tool (viewing tool 104) to delete/destroy the decryption key after the encrypted segment of electronic information is decrypted. The decrypted electronic information is also destroyed once it is displayed on the viewing tool 104. It is important to note that Giroux et al. teaches that a next decryption key for a next encrypted segment of electronic information is not delivered to a customer until customer requests the next decryption key after the decryption of the current

encrypted segment is completed,, the decrypted information is displayed and the current decryption key has been deleted.

Feig et al alone or in combination with Giroux however does not at least teach or suggest a method which:

for each encrypted section:

receiving a respective decryption key in respect of the encrypted section before playback of a preceding encrypted section is complete; decrypting and playing back the encrypted section using the respective decryption key; and destroying the respective decryption key only after at least a respective decryption key in respect of a next encrypted section has been received, such that contiguous playback of the encrypted sections of video data content is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of video data content.

Moreover, the missing claimed elements from Feig et al and Giroux et al are not found in a reasonable number of reference(s). Yet even if the missing claimed elements were found in a reasonable number of references, a person of ordinary skill in the art at the time the invention was made would not have been motivated to include these missing elements in an embodiment in the Feig's disclosure because: such would have changed the basic working principles and the operation of Feig et al which is silent on receiving a respective decryption key in respect of the encrypted section before playback of a preceding encrypted section is complete; decrypting and playing back the encrypted section using the respective decryption key; and destroying the respective decryption key only after at least a respective decryption key in respect of a next encrypted section has been received, such that contiguous playback of the encrypted sections of

video data content is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of video data content

5. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. The prior arts made of record and not relied upon is considered pertinent to applicants disclosure.

- Peterka et al (U.S. Patent Application Publication No. 2002/0170053 A1) discloses ECM and EMM Distribution for multimedia multicast content.
- Watanabe (U.S. Patent No. 7,114,073 B2) discloses digital content generating apparatus and digital content reproducing apparatus.
- Granger et al (U.S. Patent No. 6,334,189 B1) discloses the use of pseudocode to protect software from unauthorized use.
- Batty (U.S. Patent Application No. 2002/0107701 A1) discloses systems and methods for metering content on the internet.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles C. Agwumezie whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin Hewitt can be reached on **(571) 272 – 6709**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Charlie C Agwumezie/
Primary Examiner, Art Unit 3685
August 12, 2010